Program Cyber Security Plan
Exhibit 3 - Continuous Monitoring Program for Unclassified Systems

____

1.0 Purpose

The purpose of this document is to provide the Office of Science (SC) consistent methods to periodically and continuously monitor, test and evaluate the information system security controls to ensure that the controls are effectively implemented. The results of the different methods of monitoring will be combined to provide both an SC-wide and a site cyber security posture. Continuous monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program as defined by NIST SP 800-37, *"Guide for Security Certification and Accreditation of Federal Information Systems"*.

2.0 Responsibilities

The roles and responsibilities for implementing this document are described in the Office of Science Program Cyber Security Plan (PCSP).

3.0 PCSP Operation

3.1 Overview

The Office of Science implements continuous monitoring activities in accordance with the Federal Information Security Management Act (FISMA) to protect its information and information systems utilizing the principles and functions of NIST. SC staff (defined but not limited to the aforementioned roles and responsibilities): 1) ensure continuous monitoring requirements are followed; 2) ensure that continuous monitoring requirements are placed into contracts; 3) provide oversight of contractors' continuous monitoring of work planning and controls; 4) integrate continuous feedback and improvement mechanisms into their work; and 5) perform the necessary oversight and assessments of both the Federal and contractor staff.

The PCSP addresses the requirements for SC personnel in the relevant aspects of cyber security and performance of continuous monitoring functions that are Federal responsibilities. Furthermore, the PCPS serves to ensure that continuous monitoring requirements and methods of accomplishment are identified, communicated and implemented by both SC staff and contractors. This includes the oversight, assessment and evaluation of both Federal staff and contractor performance, and reporting of continuous monitoring performance data to SC and other entities (e.g., U.S. Department of Energy [DOE] and, as appropriate, Federal, state, and local governments). Effective implementation of the PCSP will ensure the security of information and the information systems for the Office of Science. Continuous monitoring and status reporting is a fair and balanced process leveraging the knowledge of the Science Information Officer in combination with the Integrated Service Centers.

The processes for addressing contractor PCSP performance expectations are outlined in the M&O Contracting Management System Description.

3.2 Key Functions/Services and Processes

The Office of Science implements continuous monitoring of their cyber security posture through a multi-level approach. This multi-level approach uses periodic site reviews, SC-wide and site cyber security metrics, and status reports to monitor performance. At the beginning of each year, the Science Information Officer will present a plan to the Chief Operating Officer (COO) for continuous monitoring of the cyber security posture of the Federal sites and laboratories. This plan will provide a schedule for site reviews, metrics, and status reporting. It will be coordinated with the Integrated Service Centers.

3.2.1 Site Review Initiative

The site review process is where representatives from SC conduct a review of the security controls and the information and information systems environment at each laboratory or site office. This review consists of in-depth interviews with personnel responsible for the security of information, and a review of cyber security documentation to assure that changes are being properly analyzed, tested and incorporated. Technical controls will be reviewed to assure they are performing as intended and represent the most secure posture suitable for mission requirements. The continuous monitoring of security controls can be accomplished in a variety of ways including independent security reviews, self-assessments, penetration testing, scanning and vulnerability assessment, or audits. The site review will verify that configuration management baselines are implemented and current, and documentation has been updated to reflect any changes.

The Office of Science expects to conduct a site review for each laboratory or site office annually. The Science Information Officer (SIO) will coordinate the site reviews with the Integrated Service Centers.

3.2.1.1 Configuration Management

Configuration Management (CM) implies administration, technical direction, and surveillance to identify and document functional and physical characteristics of an information system (or devices on a system). This means that at a detailed level changes to a system (or system devices) must be tracked and documented, and a process for approving changes and verifying compliance with specified requirements implemented. CM ensures the security protection features approved for an information system have been systematically implemented and are maintained. This is accomplished by controlling the implementation or operations of systems and the processes for system maintenance or modification. Under the configuration management task the following would be reviewed for the devices that constitute the information system infrastructure:

- Configuration baselines of workstations, servers, and network equipment – assure that the CM baseline is appropriate and maintained;
- Patch management is being implemented consistent with the Cyber Security Program Plan (CSPP); and
- Inventory tracking is being implemented consistent with the CSPP.

3.2.1.2 Documentation of Information System Changes

An information system will typically be in a constant state of migration with upgrades to hardware, software, or firmware, and possible modifications to the system environment. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation. The objective of the configuration management and control task at the system level is to:

- Document the proposed or actual changes to the information system;
- Determine the impact of proposed or actual changes on the security of the system; and
- Document major applications or general support systems added to the infrastructure.

SC is responsible for ensuring that any relevant information about the specific proposed or actual changes to the hardware, firmware, or software, (such as version or release numbers, descriptions of new or modified features or capabilities, and security implementation guidance), is recorded. It is also important to record any changes to the information system environment, such as modifications to the facility. The information system owner and Information Security Officer (ISO) should use this information in assessing the potential security impact of the proposed or actual changes to the information system. Significant changes to the information system should not be undertaken prior to assessing the security impact of such changes.

3.2.2 Metrics

3.2.2.1 Metrics Collection

The Office of Science has developed SC-wide metrics to provide a global view of the cyber security posture of science activities at Federal sites and the laboratories. It is expected that SC-wide metrics will be gathered annually. Site metrics, illustrating the cyber security posture of a specific site, will be gathered on a quarterly basis. Both sets of initial metrics are shown in Section 5.0 of this document. They may be adjusted to address new issues or changes in policy as they arise.

The Science Information Officer will coordinate with the Integrated Service Centers as to how and when the metrics will be gathered, analyzed, and presented to management.

Efforts will be made to gather information from existing sources and pre-populate the metrics before transmitting them to the Federal sites and laboratories.

3.2.2.2 Site Metrics

The objective of the site metrics is to select an appropriate set of security controls that reflect the security posture of the information systems within a laboratory, site office or HQ. The continuous monitoring of security controls helps to identify potential security-related problems in the information system that are not identified during the site review process conducted as part of the configuration management and control process.

These metrics assure that the laboratories, site offices, Integrated Service Centers, and SC Headquarters regularly review/analyze audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, report findings to the appropriate officials, and takes necessary corrective actions.

The criteria established by SC and the information system owners in the selection of security controls to be monitored, reflect the organization's priorities and the importance of the information system to the Department. For example, certain security controls are considered more critical than other controls because of the potential impact on the information system if those controls were subverted or found ineffective. The security controls being monitored will be periodically reviewed to ensure that a representative sample of controls which best reflects the security posture of facilities is included in the ongoing security assessments.

3.2.3 Monthly Status Reporting and Documentation Update

Status reporting and documentation are key elements of a robust cyber security program, and provide the primary artifacts that the controls in place work. SC is committed to ensure documentation of required lists and that configuration standards are maintained. Policies and procedures used to inform personnel on the proper use of information and information systems should be readily available for reference.
Monthly cyber security status reports will be delivered to the Laboratory Director who will transmit the reports to the Site Office Manager, DAA, the Manager of the Integrated Service Center (which has cognizance over that specific site or laboratory), and the Science Information Officer. The Science Information Officer will develop a consolidated status for the COO.

The objectives of the status reporting task are to:

- Ensure that the CSPP is updated to reflect proposed or actual changes to the information system.
- Ensure that the Plan of Action and Milestones is updated to reflect the activities carried out during the continuous monitoring phase.

- Report the security status of the information system and changes to the risks to the DAA and Site/Laboratory Management.
- Ensure that cyber security is responsive to evolving threats and vulnerabilities.
- Highlight any cyber security incidents, issues identified during audits, inspections, or self assessments, and disseminate the approach to their remediation throughout SC.

4.0 Requirements

The following summarizes high-level requirements relevant to the PCSP.

P.L. 103-356, Government Management Reform Act of 1994, (October 13, 1994)

P.L. 104-208, Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996)

P.L. 104-231, Electronic Freedom of Information Act (e-FOIA), (October 2, 1996)

P.L. 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002)

P.L. 93-579, Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974)

P.L. 96-349, Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002)

P.L. 97-255, Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)

P.L. 99-474, Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16, 1986)

P.L. 99-508, Electronic Communications Privacy Act of 1986, (October 21, 1986)

P.L. 100-235, Computer security Act of 1987, (January 8, 1988)

P.L. 104-106, Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996)

OMB Circular A-123, Management Accountability and Control, (August 4, 1986) (revised Dec 21, 2004)

OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, (November 2003)

OMB Memorandum M-96-20, Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)

OMB Memorandum M-97-02, Funding Information Systems Investments, (October 25, 1996)

OMB Memorandum M-99-05, Instructions for Complying With the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records", (January 7, 1990)

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, (June 2, 1999)

OMB Memorandum M-99-20, Security of Federal Automated Information Resources, (June 23, 1999)

OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, (June 22, 2000)

OMB Memorandum M-00-015, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, (December 20, 2000)

OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)

OMB Memorandum M-01-26, Component-Level Audits, (July 10, 2001)

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (September 30, 2003)

OMB Memorandum M-04-04, E-Authentication Guidance, (December 16, 2003)

OMB Memorandum M-04-25, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)

OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology, (September 8, 2004)

OMB Memorandum M-05-02, Financial Management Systems, (December 1, 2004)

OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, (December 17, 2004)

OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, (February 11, 2005)

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, (May 22, 2006)

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, (June 23, 2006)

OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments, (July 12, 2006)

NIST Federal Information Processing Standard (FIPS) 201-1, National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)

NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, (March 2006)

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

NIST FIPS 142-2, Security requirements for Cryptographic Modules, (May 2001)

NIST Special Publication [1](SP) 800-92, Guide to Computer Security Log Management, (September 2006)

NIST SP 800-88, Guidelines for Media Sanitization, (September 2006)

NIST SP 800-83, Guide to Malware Incident Prevention and Handling, (November 2005)

NIST SP 800-73, Rev. 1, Interfaces for Personal Identity Verification, March 2006 (updated April 20, 2006)

NIST SP 800-70, The NIST Security Configuration Checklists Program, (May 2005)

[1] Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, (January 2005)

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)

NIST SP 800-61, Computer Security Incident Handling Guide, (January 2004)

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)

NIST SP 800-55, Security Metrics Guide for Information Technology Systems, (July 2003)

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)

NIST SP 800-53, Rev. 1, Recommended Security Controls for Federal Information Systems, (December 2006)

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, (October 2003)

NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, (November 2002)

NIST SP 800-47, Security Guide for Interconnecting Information Technology System, (August 2002)

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, (June 2002)

NIST SP 800-30, Risk Management Guide for Information Technology Systems, (July 2002)

NIST SP 800-26, Rev. 1, Guide for Information Security Program Assessments and System Reporting Form, (November 2001)

NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

DOE P 205.1, Departmental Cyber Security Management Policy, (May 8, 2001)

DOE O 205.1A, Department of Energy Cyber Security Management Program, (December 4, 2006)

DOE 0 221.2, Cooperation with the Office of Inspector General, (March 22, 2001)

DOE P 226.1, Department of Energy Oversight Policy, (June 10, 2005)

DOE 0 226.1, Implementation of Department of Energy Oversight Policy, (September 15, 2005)

DOE P 470.1, Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)

DOE 0 470.2B, Independent Oversight and Performance Assurance Program, (October 31, 2002)

DOE 0 471.1, Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)

DOE 0 470.4, Safeguards and Security Program, (August 26, 2005)

DOE 0 475.1, Counterintelligence Program, *(*February 10, 2004)

E.O. 12344, Naval Nuclear Propulsion Program, (February 1, 1982)

E.O. 12958, Classified National Security Information, (April 17, 1995)

E.O. 13011, Federal Information Technology, (July 17, 1996)

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004)

5.0 Subject Areas

5.1 SC Cyber Security Metrics – SC-Wide Metrics

These metrics are designed to measure SC-wide cyber security posture by reflecting the Director's cyber security performance standards in the May 3, 2006 memorandum on "Cyber Security Risk in the Science Community". In addition, they meet the requirements for program specific, performance-based metrics as set forth in DOE O 205.1A, *Department of Energy Cyber Security Management Program*.

5.1.1 Policy Metrics

- Organization (Federal facility or laboratory) self-reporting with letter grade (A-F) on completeness of full range of policy documents implementing NIST SP 800-53 controls (either written or identified as tasks in the Plan of Action and Milestones).
- Self-reported letter grade on whether the Program Cyber Security Plan is current and reflects national and Departmental policy.

5.1.2 Skills Metrics

- The percentage and number of users that attended cyber security awareness training in the last 12 months.
- The percentage and number of System Administrators who attended specialized training in the last 12 months (this could later be changed to System Administrators with certification once a certification program is fielded).
- The percentage and number of Designated Approving Authorities that attended specialized training in the last 12 months.

5.1.3 Integration Metrics

- The percentage and number of systems/enclaves with current certification and accreditation documentation at each site and laboratory (Federal and contractor).
- The percentage and number of sites and laboratories (Federal and contractor) with an approved Authority to Operate, based on NIST 800-53 controls.
- The percentage and number of sites with a deployed architecture to protect personally identifiable information.

5.1.4 Management Metrics

- The percentage and number of sites and laboratories (Federal and contractor) with threat statements, risk assessments, cyber security plans, and POA&Ms updated or reviewed within the last 12 months.

- The percentage and number of sites and laboratories (Federal and contractor) with threat statements, risk assessments, cyber security plans, and POA&Ms that reflect current infrastructure and operating processes.
- The percentage and number of sites and laboratories (Federal and contractor) with Plan of Actions and Milestones on schedule.
- The percentage and number of sites and laboratories (Federal and contractor) that have reported cyber incidents or a negative report (no cyber incidents) to the proper organizations or personnel in a timely manner.
- The number of network and system/enclave external and internal penetrations per site detected during technical testing related to the performance of a Continuous Monitoring Initiative.

5.2 SC Cyber Security Metrics – Site Metrics

These metrics are used to measure the cyber security posture at each site.

5.2.1 Organizational Strength

Explanation of Metric: This metric attempts to determine if the site has adequate IT staff members to implement controls and maintain a strong cyber security program. The metric also makes an assessment whether the head of the cyber organization has sufficient visibility within the management chain to carry out the organizational goals of the Office of Science. If the head of the cyber security staff reports directly to the Lab Director, this is considered desirable. Reporting further down the organization is considered less desirable.

What we look at:

1. Strength of the individuals in the CIO organization (weak, adequate, strong)
2. Extent of resources for cyber security (staff, budget, etc.) (insufficient/adequate)
3. Extent to which CIO (and cyber security organization) reports to the Lab Director (yes/no, is it a direct report, levels of management)

5.2.2 Authentication

Explanation of Metric: Access to the networks needs to be controlled to assure that only those individuals who have a need are granted access. Control is enforced by having the access points into the network under the management of the site's IT staff and by requiring all users to authenticate themselves via passwords, tokens or other devices'.

Access to moderate controlled information and administration systems both locally and remotely:

- locally
  - (**adequate)** Kerberos and DOE/strong passwords, (**better**) Kerberos and tokens, (**best**) Personal Identity Verification (PIV) access

- remotely
  - Secure Shell 2 (SSH2) and DOE/strong password, SSH2 and tokens

5.2.3 Network

Explanation of Metric: Networks that are not segmented are extremely vulnerable because a compromise of any one device places the entire infrastructure at risk. Highly segmented infrastructures are rated higher than flatter networks.

Segmentation or controls are implemented so that the compromise of any one enclave or subnet does not compromise other enclaves or other subnets on the campus.

Degree of Segmentation:

- (**flat – weak**) border firewall only,
- (**better**) ACL, routers and firewalls,
- (**best**) V-LANS, routers, ACLs and firewalls

5.2.4 Log Review/History

Explanation of Metric: A key tool in the reconstruction of a "cyber incident" is a review of logs for the devices that were compromised. In order to assure that this tool can be applied, it is essential that the logging feature is active for as many devices as possible and that the log files are regularly reviewed. Filtering software to look for suspicious activity (usage late at night or during the weekend) may alert the IT staff before a compromise occurs or help identify a compromised system. This metric has multiple parts: the percentage of devices that have logging enabled; the application of filtering software to look for abnormalities; and the regular (actual "eyes-on" people) review of log files.

1. percentage of servers and workstations that forward to a central log (percentage)
2. existence of filtering tools to look for abnormalities (yes/no)
3. systematic periodicity of log review (daily, weekly, monthly, longer than monthly)

5.2.5 Incident Response

Explanation of Metric: One of the benefits of having a system scan and patch the management program is that if a device is compromised, the extent of the threat is limited. When a security breech occurs, multiple devices are usually affected. This metric measures the number of devices compromised for each cyber security incident at a site. The metric also seeks to gauge the speed at which the incident is detected (e.g., time of attack to when the attack is alerted). It also seeks to determine how long it takes for the corrective action(s) to be completed. The ideal score is “0” (no devices were compromised).

There are two types of incidents:

- Type 1: attack is successful – at least one device was compromised
- Type 2: attack is unsuccessful – site was scanned but no further damage

The goal is not to have any Type 1 attacks for this metric. This metric also serves to measure how effective the Intrusion Prevention System (IPS) and Intrusion Detection Systems (IDS) are. For example, attacks which are detected quickly are considerably less problematic than attacks which continue undiscovered for weeks or months.

1. Number of systems affected by a specific attack (number)
2. Type of incident (number of Type 1 and 2)
3. Timeframe in which the incident is detected (hours/days, days/weeks)
4. Timeframe in which the incident is mitigated (hours/days, days/weeks)

5.2.6 Network Scanning

Explanation of Metric: The first level of defense is to assure that all required patches to the operating systems are applied and that all signature files are updated. In order to accomplish this task, all network devices should be scanned to assure they are current and that updates have been applied. Since vulnerabilities and viruses require constant vigilance, the more frequent scanning and updating is accomplished, the better this defense layer is. This metric measures how often the scanning is done as well as the number of devices that are being scanned. Devices which cannot be scanned or updated should be isolated from the network via a firewall.

1. Percent of systems scanned continuously (percentage)
2. Frequency and comprehensiveness of deep scans (frequency and percentage of deep scans)
3. Existence of compensating controls (yes/no)

5.2.7 Patching

Explanation of Metric: This metric is the companion metric to network scanning. One of the purposes of scanning is to identify devices and applications that are not current with updated security patches. Patches that are applied on a timely basis result in the most robust implementation of this control. This metric measures the number of devices that are patched and the speed at which the patches are applied.

1. Number of systems at current patch level with current virus signature files (percentage)
2. Response time per level of patch criticality (response time - hrs/days, days/wks)

5.2.8 Configuration Management

Explanation of Metric: Management of the infrastructure is facilitated when standard configurations are implemented across as many devices as possible. Having a standard configuration allows the site or facility IT organization to distribute and implement group policies to user workstations, servers, and network equipment to facilitate management of the facility. Implementation of a standard configuration (e.g. CIS level 1 benchmarks) promotes management involvement and oversight for addressing changes to the configuration, if this is required.

The metric looks at the number of systems that implemented a recognized national standard (NIST checklist, Center for Internet Security, National Security Agency) within their infrastructure. Sites that have implemented a standard configuration on the greatest number of devices possible are considered robust for this metric. Reducing the possibility of user's making their own changes is also considered in this metric – sites will be weighed as to whether they have controls which either flag configuration changes or prevent configuration changes.

1. Evidence of national standards (percentage of devices with a national standards applied)
2. Number of operating environment systems (one, few, many)
3. Age of operating environment systems (percentage currently supported)
4. Restriction of administrative rights (least number of administrators/many administrators)

5.2.9 Sensitive and Personally Identifiable Information (PII) Systems Protections

Explanation of Metric: PII is to be protected by moderate controls. Users requiring access to PII must be uniquely identified and authenticated using strong methods. PII must also be protected in transit and storage via secured communications channel (SSH2) or encyrption. Two factor authentication is the preferred method for access to systems containing PII.

The metric measures the level of access enforcement to PII. Sites should require two factor authentication (especially via remote access), provide a secure communications channel, have encryption software and assure PII is not stored in the clear.

1. Two factor authentication to PII enforced (yes/no)
2. All PII are protected at moderate controls (yes/no)
3. PII in storage is encrypted (yes/no)

4. A secured communication channel used when transmitting PII (yes/no)

5.2.10 Classified Systems Protections

Explanation of Metric: Access to classified information and information systems must be strictly controlled. This includes not only electronic information but also printed information. This metric measures the level of protection to the information and information systems at the facility. Currently, all sites by virtue of their current ATO have been rated satisfactory for all aspects of this metric. More details on this metric may evolve once the classified program is initiated.

1. Mandatory access control is strictly enforced (yes/no)
2. Media handling procedures/restrictions enforced (yes/no)
3. Physical controls enforced (yes/no)

5.2.11 Security Awareness Training

Explanation of Metric: If personnel with cyber security responsibilities such as privileged users are not given appropriate security awareness training, a site may not be equipped to combat the latest threats and vulnerabilities. Many sites have privileged users, but do not provide training for these users so they understand the responsibility that goes along with these privileges. Privileged users have the ability to cause more (inadvertent) harm to the system than users with limited rights because they have the ability to change the configuration settings of their equipment.

This metric credits those sites that require all people with system administration rights to take a system administration class. The metric also tries to determine the effectiveness of the awareness training provided at each site by tracking the number of incidents that are cause by “user carelessness” (e.g., downloaded a Trojan from a phishing site). Sites that require specialized training for system administrators, and have “low” user-error incidents are considered robust for this metric.

1. Security awareness training provided (percentage in last year)
2. System administrator training is required for all individuals with system administrative rights (percentage in last year)
3. Number of “user error” incidents/number of users (number/ratio)

6.0 References

The following summarizes high-level references relevant to the PCSP.

OMB Circular A-123, Management Accountability and Control, (August 4, 1986), revised (Dec 21, 2004)

OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, (November 2003)

OMB Memorandum M-96-20, Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)

OMB Memorandum M-97-02, Funding Information Systems Investments, (October 25, 1996)

OMB Memorandum M-99-05, Instructions for Complying With the President's Memorandum of May 14, 1998, “Privacy and Personal Information in Federal Records”, (January 7, 1990)

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, (June 2, 1999)

OMB Memorandum M-99-20, Security of Federal Automated Information Resources, (June 23, 1999)

OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, (June 22, 2000)

OMB Memorandum M-00-015, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)

OMB Memorandum M-01-26, Component-Level Audits, (July 10, 2001)

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (September 30, 2003)

OMB Memorandum M-04-04, E-Authentication Guidance, (December 16, 2003)

OMB Memorandum M-04-25, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)

OMB Memorandum M-04-26, Personal Use Policies and “File Sharing” Technology, (September 8, 2004)

OMB Memorandum M-05-02, Financial Management Systems, (December 1, 2004)

OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, (December 17, 2004)

OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, (February 11, 2005)

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, (May 22, 2006)

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, (June 23, 2006)

OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments”, (July 12, 2006)

NIST Federal Information Processing Standard (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)

NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, (March 2006)

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

NIST FIPS 142-2, Security requirements for Cryptographic Modules, (May 2001)

NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management, (September 2006)

NIST SP 800-88, Guidelines for Media Sanitization, (September 2006)

NIST SP 800-83, Guide to Malware Incident Prevention and Handling, (November 2005)

NIST SP 800-73, Rev. 1, Interfaces for Personal Identity Verification, March 2006, (updated April 20, 2006)

NIST SP 800-70, The NIST Security Configuration Checklists Program, (May 2005)

NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, (January 2005)

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)

NIST SP 800-61, Computer Security Incident Handling Guide, (January 2004)

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)

NIST SP 800-55, Security Metrics Guide for Information Technology Systems, (July 2003)

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)

NIST SP 800-53, Rev.1, Recommended Security Controls for Federal Information Systems, (December 2006)

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, (October 2003)

NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, (November 2002)

NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, (August 2002)

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, (June 2002)

NIST SP 800-30, Risk Management Guide for Information Technology Systems, (July 2002)

NIST SP 800-26, Rev. 1, Guide for Information Security Program Assessments and System Reporting Form, (November 2001)

NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

DOE Chief Information Officer Guidance – Cyber Security

CS-01, Management, Operational, and Technical Controls Guidance, (July 6, 2006)

CS-02, Certification and Accreditation, (March 24, 2006)

CS-03, Risk Management, (June 30, 2006)

CS-04, Vulnerability Management, (July 31, 2006)

CS-05, Interconnect Agreements, (July 31, 2006)

CS-06, Plans of Actions and Milestones (POA&M), (September 07, 2006)

CS-07, Contingency Planning, (August 26, 2006)

CS-08, Configuration Management, (November 27, 2006)

CS-09, Incident Management, (January 2007)

CS-11, Clearing and Media Sanitization, (January 2007)

CS-12, Password Management, (June 30, 2006)

CS-13, Wireless Devices and Information Systems, (June 30, 2006)

CS-14, Portable/Mobile Devices, (January 2007)

CS-15, Personally Owned Devices, (January 2007)

CS-18, Foreign National Access to DOE Information Systems, (January 2007)

CS-20, INFOCON, (December 06, 2006)

CS-23, Peer-To Peer Networking,(December 2006)

CS-24, Remote Access, (January 2007)

CS-37, Security, Testing and Evaluation, (January 2007)

CS-38A, Protection of Sensitive Unclassified Information, including Personally Identifiable Information, (November 2006)